ZUORA

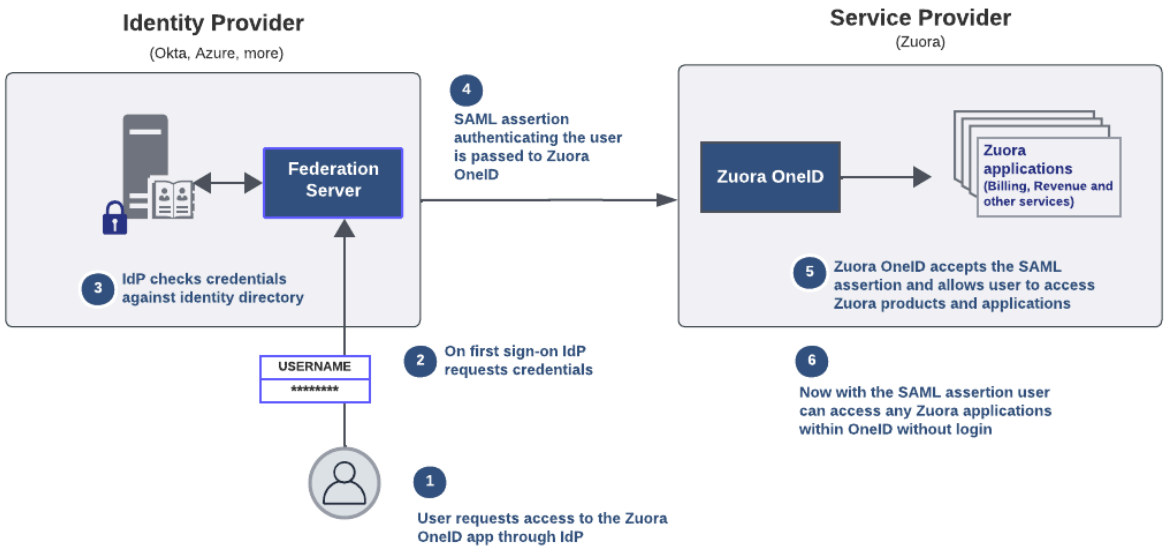
# Zuora OneID

ZUORA

Table of content

# Overview

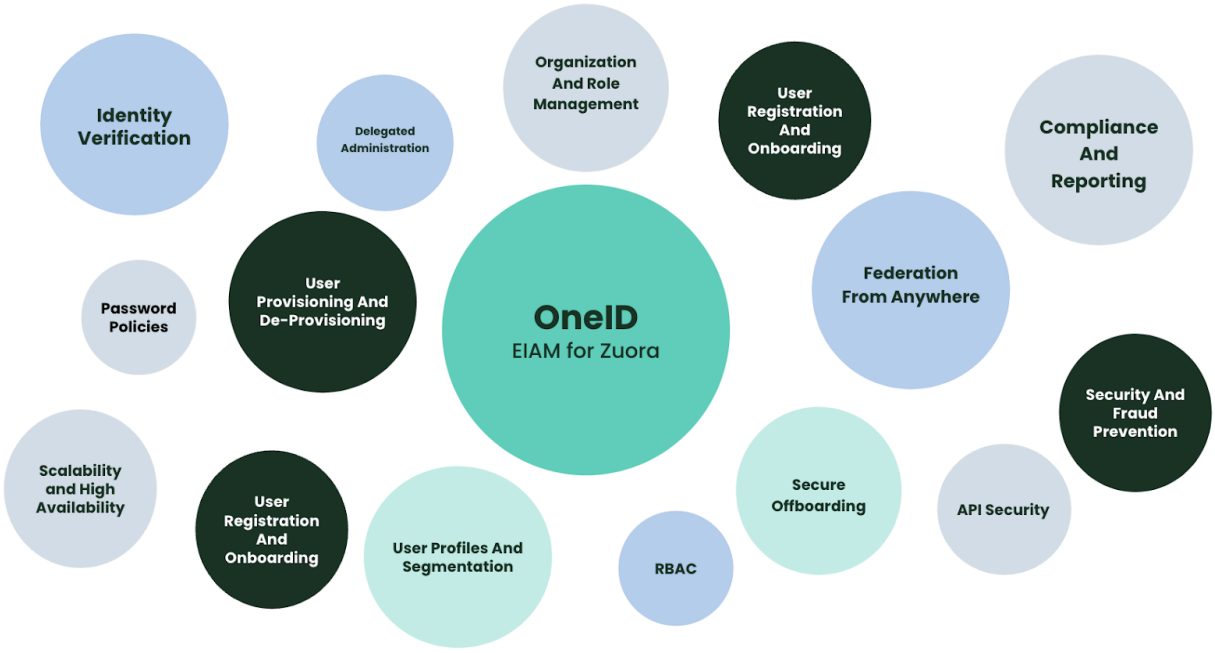
Zuora OneID is a robust identity and access management (IAM) platform designed to enhance security and streamline user access across various Zuora applications and services. Zuora OneID is a specialized solution for Zuora applications, offering a comprehensive approach to managing employee identities and overseeing their activities within Zuora environments, ensuring compliance with regulatory standards. To know more, take a look at the Overview of Zuora OneID video.




For more information about how to get started, see Get started with OneID.

# Key feature highlights

The importance of onboarding with Zuora OneID is emphasized by the following essential features and use cases.




## Seamless Single Sign-On (SSO) Integration

Zuora OneID features Single Sign-On functionality, enabling users to access multiple applications with a single set of credentials. By reducing the need for multiple usernames and passwords, this not only enhances security but also improves user experience. With Zuora OneID, you can enjoy IdP-initiated SSO using the SAML 2.0 protocol and effortlessly connect with leading Identity Providers (IdP) such as Okta, Azure AD, Google, Redhat, OneLogin, and more.

## Universal Identity

Zuora OneID acts as a centralized repository for user profiles and identity information across various Zuora applications and services. With a single set of credentials, you can effortlessly access multiple Zuora tenants, eliminating the need to remember and manage multiple passwords.

## User Lifecycle Management

From start to finish, Zuora OneID oversees the entire lifecycle of user identities, including onboarding and offboarding. This involves managing user provisioning,

de-provisioning, and profiles across multiple Zuora applications to ensure effective and secure user identity management.

## Authorization and Access Policies

Organizations can use Zuora OneID to establish and enforce access policies through security or user groups, guaranteeing appropriate access levels for users according to their roles. Security groups enable users to simultaneously hold different roles across multiple Zuora applications.

## Automated User Provisioning

Zuora OneID facilitates secure automation of user identity data exchange between service providers and Zuora through SCIM APIs. The cost and complexity of user management operations are reduced through this integration.

## Security and Compliance

Zuora OneID ensures compliance with industry security standards and certifications. With aggregated data across all Zuora applications, organizations can effortlessly monitor user and role creations, assignments, and access details for auditing purposes.

# Get Started with OneID

The following key configurations are necessary to set up to begin using Zuora OneID.

## 1. Create an account in OneID

a. Contact the support team and share Zuora tenant IDs to map them to your organization.
b. Activate the user account from the activation email sent to you.

## 2. Set up Single Sign-On

a. Contact your IT team to create a custom SAML app for Zuora OneID in your Identity Provider (IdP). Currently, Zuora OneID enables IdP-initiated SSO support. You must click and use the custom SAML app from your IdP to log in to Zuora. This is a one-time IdP integration for all of your Zuora tenants.
b. Refer to configure IdP initiated Single Sign-On with Zuora if you are using Azure as your IdP.
c. After creating the custom SAML app for Zuora OneID in your IdP, copy the metadata URL and paste it into the OneID settings. Refer to Manage single sign-on configurations for more information.
d. Map the federated ID of users for SSO to work.

## 3. Setup user roles for Zuora tenants

a. Navigate to the User Roles module in OneID and select a tenant before creating or importing the roles for that tenant.
b. You can either create new user roles in OneID or you can migrate your existing roles that are defined in the tenant
c. Create or import the roles for all your available tenants before mapping them to the users.
d. Rename migrated roles in OneID according to department, designation, or user groups with the same access levels. For more information on user roles in OneID, see Manage User roles in OneID.
e. A single role must be assigned to a user for any given tenant in OneID's unified set of user roles, which includes all modular roles for each billing application module.

## 5. Setup User Groups

a. Create user groups with tenants configured to resemble the security groups in your AD or the user profiles in your organization.
b. Assign single or multiple tenants per group with a OneID role assigned to every tenant.

c. For more information, see Manage user and group provisioning in OneID.

## 6. Onboard users to OneID

OneID automatically sends activation emails to new users when they are added. For more information, see Add users to OneID. You can also add the User Groups to the users while creating their accounts in OneID.

## 7. Assign user access to Zuora applications

User Groups is the go-to solution to automate user provisioning or bulk user provisioning in Zuora. OneID allows for the formation of user groups that mimic your AD groups or security groups in your IdP. Additionally, you can automate the user provisioning in Zuora using SCIM or User Management APIs in OneID.

Enable tenants and assign roles to them before adding users to the Groups. To manage user access through groups, refer Manage user provisioning with User Groups.